

WHAT IS CLAIMED IS:

1           1.    An access control method for verifying a user's  
2    access to a network, comprising the steps:

3                upon receiving an indication signifying that  
4    said user is attempting to access said network using a  
5    multimedia appliance, invoking a multimedia session  
6    engine to launch a network access application;

7                interrogating said user by an access  
8    application server associated with said network;

9                receiving a multimedia response from said user  
10   responsive to said interrogating step;

11               determining if said multimedia response is  
12   valid; and

13               if so, granting permission to said user with  
14   respect to accessing said network.

1           2.    The access control method for verifying a  
2    user's access to a network as set forth in claim 1,  
3    wherein said user is remotely located with respect to  
4    said network.

1           3.    The access control method for verifying a  
2    user's access to a network as set forth in claim 2,  
3    wherein said multimedia response from said user comprises  
4    an audio response responsive to said interrogating step.

1           4. The access control method for verifying a  
2 user's access to a network as set forth in claim 2,  
3 wherein said multimedia response comprises a video input  
4 of said user in response to said interrogating step.

1           5. The access control method for verifying a  
2 user's access to a network as set forth in claim 4,  
3 wherein said video input comprises a live picture of said  
4 user.

1           6. The access control method for verifying a  
2 user's access to a network as set forth in claim 2,  
3 further comprising the steps:

4               upon granting permission to said user with  
5 respect to accessing said network, re-interrogating said  
6 user after a time period;

7               receiving a response from said user responsive  
8 to said re-interrogating step; and

9               if said response from said user not valid,  
10 terminating said user's access to said network.

1           7. The access control method for verifying a  
2 user's access to a network as set forth in claim 6,  
3 wherein said response from said user comprises at least  
4 one of an audio response, a video input, a device input  
5 effectuated via said multimedia appliance, and a  
6 biometric ID input of said user.

1           8.    The access control method for verifying a  
2   user's access to a network as set forth in claim 7,  
3   wherein said network comprises a corporate computer  
4   network, and further wherein said re-interrogating step  
5   is effectuated by a human operator associated with said  
6   corporate computer network.

1           9.    The access control method for verifying a  
2   user's access to a network as set forth in claim 7,  
3   wherein said network comprises a corporate computer  
4   network, and further wherein said re-interrogating step  
5   is effectuated by an automated access control apparatus  
6   associated with said corporate computer network.

1           10.   The access control method for verifying a  
2   user's access to a network as set forth in claim 7,  
3   wherein said network comprises a home network, and  
4   further wherein said re-interrogating step is effectuated  
5   by an access control application server associated with  
6   a public network that serves said user.

1           11. An access control system for use with a  
2 multimedia-capable next-generation network, said system  
3 for providing remote access to a network portion,  
4 comprising:

5                 means for receiving an indication signifying  
6 that a remotely located user is attempting to access  
7 said network portion using a multimedia appliance;

8                 a multimedia session engine operable to invoke  
9 a network access application, responsive to said  
10 indication, on an access application server associated  
11 with said multimedia-capable next-generation network;

12                means for interrogating said remotely located  
13 user for a multimedia response, said means for  
14 interrogating operating responsive to control inputs  
15 provided by said multimedia session engine;

16                logic means, associated with said access  
17 application server, for determining if said multimedia  
18 response from said user is valid; and

19                means for granting permission to said user with  
20 respect to accessing said network portion, provided said  
21 multimedia response has been determined to be valid.

1           12. The access control system for use with a  
2 multimedia-capable next-generation network as set forth  
3 in claim 11, wherein said network portion comprises a  
4 network selected from the group consisting of a corporate  
5 network, a home network, a small business network, and a  
6 private enterprise network.

1           13. The access control system for use with a  
2 multimedia-capable next-generation network as set forth  
3 in claim 12, wherein said multimedia response comprises  
4 at least one of an audio response, a video input, a  
5 device input effectuated via said multimedia appliance,  
6 and a biometric ID input of said user.

1           14. The access control system for use with a  
2 multimedia-capable next-generation network as set forth  
3 in claim 13, further including means for re-interrogating  
4 said remotely located user after a select time period  
5 upon granting permission to access said network portion.

1           15. The access control system for use with a  
2 multimedia-capable next-generation network as set forth  
3 in claim 13, wherein said means for interrogating said  
4 remotely located user includes means for effectuating  
5 different levels of interrogation depending upon a  
6 plurality of access levels allowed with respect to said  
7 network portion.

1           16. A computer-accessible medium operable with a  
2 network element disposed in a multimedia-capable next-  
3 generation network, said computer-accessible medium  
4 carrying a sequence of instructions which, when executed  
5 by at least one processing entity associated with said  
6 multimedia-capable next-generation network, cause said  
7 network element to perform the following steps:

8           upon receiving an indication signifying that a  
9 user is attempting to access a network portion using a  
10 multimedia appliance, invoking a multimedia session  
11 engine to launch a network access application;

12           directing an access application server  
13 associated with said multimedia-capable next-generation  
14 network to interrogate said user;

15           receiving a multimedia response from said user  
16 responsive to said interrogating step;

17           determining, in said access application server,  
18 if said multimedia response is valid; and

19           if so, granting permission to said user with  
20 respect to accessing said network portion.

1           17. The computer-accessible medium operable with a  
2 network element disposed in a multimedia-capable next-  
3 generation network as set forth in claim 16, wherein said  
4 network portion comprises a network selected from the  
5 group consisting of a corporate network, a home network,  
6 a small business network, and a private enterprise  
7 network.

1           18. The computer-accessible medium operable with a  
2 network element disposed in a multimedia-capable next-  
3 generation network as set forth in claim 17, wherein said  
4 user is remotely located with respect to said network  
5 portion.

1           19. The computer-accessible medium operable with a  
2 network element disposed in a multimedia-capable next-  
3 generation network as set forth in claim 18, wherein said  
4 multimedia response comprises at least one of an audio  
5 response, a video input, a device input effectuated via  
6 said multimedia appliance, and a biometric ID input of  
7 said user.

1           20. The computer-accessible medium operable with a  
2 network element disposed in a multimedia-capable next-  
3 generation network as set forth in claim 19, wherein said  
4 sequence of instructions further includes instructions to  
5 carry out the following steps:

6           upon granting permission to said user with  
7 respect to accessing said network portion, re-  
8 interrogating said user after a time period;

9           receiving a response from said user responsive  
10 to said re-interrogating step; and

11           if said response from said user not valid,  
12 terminating said user's access to said network portion.



1           21. A user verification method for use in a service  
2 network for positively identifying a user attempting to  
3 gain access to a controlled facility, comprising the  
4 steps of:

5                 upon receiving an indication that said user is  
6 attempting to access said controlled facility, invoking  
7 a multimedia session engine to launch an access service  
8 application;

9                 interrogating said user by an access  
10 application server associated with said service network;

11                 receiving a multimedia response from said user  
12 responsive to said interrogating step;

13                 determining if said multimedia response is  
14 valid; and

15                 if so, granting permission to said user with  
16 respect to accessing said controlled facility in  
17 accordance with a user access profile stored on said  
18 service network.

1           22. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 21, wherein said multimedia response from  
5 said user comprises at least one of an audio response,  
6 video response, and a text response, and further wherein  
7 said controlled facility is selected from the group  
8 consisting of a corporate network, a home network, a  
9 physical area, and an access-controlled service.

1           23. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 22, further comprising the steps:

5           upon granting permission to said user with  
6 respect to accessing said controlled facility, re-  
7 interrogating said user after at least one of a  
8 predetermined time period and a predetermined user  
9 action;

10           receiving a response from said user responsive  
11 to said re-interrogating step; and

12           if said response from said user not valid,  
13 terminating said user's access to said controlled  
14 facility.

1           24. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 22, wherein said audio response comprises  
5 playing back on a multimedia appliance a stored audio  
6 file associated with said user.

1           25. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 22, wherein said audio response comprises  
5 generating a live audio file associated with said user on  
6 a multimedia appliance.

1           26. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 22, wherein said video response comprises  
5 playing back on a multimedia appliance a stored video  
6 file associated with said user.

1           27. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 22, wherein said video response comprises  
5 generating a live video file associated with said user on  
6 a multimedia appliance.

1           28. The user verification method for use in a  
2 service network for positively identifying a user  
3 attempting to gain access to a controlled facility as set  
4 forth in claim 22, wherein said multimedia response  
5 further includes providing a still photograph of said  
6 user.